GCCS System Integration Support

Technical Report/Study: Integration of Automated Message Handling System (AMHS) into the Defense Messaging System (DMS)

April 12, 1996

Prepared for:

DISA/D611
ATTN: Ms. Claire Burchell
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Contract Number: DCA100-94-D-0014
Delivery Order Number: 204, Task 2
CDRL Number: A005

Prepared by:

Computer Sciences Corporation
Defense Enterprise Integration Services
Four Skyline Drive
5113 Leesburg Pike, Suite 700
Falls Church, VA 22041

THIS DOCUMENT IS UNCLASSIFIED

TECHNICAL REPORT/STUDY INTEGRATION OF AUTOMATED MESSAGE HANDLING SYSTEM (AMHS) INTO THE DEFENSE MESSAGING SYSTEM (DMS)

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

1.0 INTRODUCTION

The Defense Messaging System (DMS) consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in the DoD. There are several such messaging functions within the Global Command and Control System (GCCS). One of these is the Automated Message Handling System (AMHS). AMHS, as well as the other GCCS messaging functions, will need to be integrated into the DMS. A study of this integration, with particular attention to possible problems, is the subject of this report.

1.1 Purpose

The purpose of the study was to identify potential problems in the integration of AMHS into DMS; problems that could prove to be costly to resolve if left unsolved until later in the program's maturity. The DMS has enormous scope and will eventually affect every aspect of electronic communications within DoD. Thus, even if the GCCS program is not immediately impacted by a particular DMS feature, the GCCS program must be aware of the future to plan in the present.

1.2 Scope

Although the formal subject of the study relates solely to AMHS integration into DMS, two factors forced a broadening of the study's scope:

- AMHS is not the only GCCS messaging function impacted by DMS requirements.
- The term “integration” is at face value misleading, given the goals and complexity of GCCS messaging.

A more practical restatement of the issue would be: “how can the total messaging requirements of the GCCS be best satisfied; within the constraints imposed by the DMS, and utilizing the assets of the DMS to full potential.” The first sentence in Section 1.0 has been used in a number of briefings, reports, and documents pertaining to the DMS program. The terms “organizations” and “individuals” should be noted here because they refer to very different and specific types of messaging capabilities, each with its particular requirements and uses. Organizational messaging refers to what we think of as Automatic Digital Network (AUTODIN) messages: formal, standard, official, etc. These require approval for transmission from someone with that specific authority. Individual messaging as used in the DMS documentation can be considered as “everything else.” Therefore, the e-mail and teleconferencing capabilities provided by the GCCS Common Operating Environment (COE) must be included in any discussion of GCCS and DMS.

This report addresses AMHS, which provides AUTODIN connectivity to GCCS Version 2.1; the e-mail and teleconferencing capabilities of the GCCS COE; and the DMS Program capabilities, practices, and procedures that will affect the GCCS messaging functions, both near-term and in the future. The expected audience is the GCCS engineering community, managers, and planners. For this reason, the GCCS in general and the GCCS AMHS in particular are not described in detail. More attention is paid to the DMS, but even there the intent is not to present a complete system description or concept of operations, both of which are available from the DMS Program Management Office. Information about both programs herein is limited to the amount and level

of detail necessary for the GCCS professional staff to see where the problems (and potential benefits) from the DMS are likely to occur.

1.3 Methodology

The following steps were taken to conduct this study:

a) Examine the two systems: all available existing documentation concerning the architectures (hardware, software, protocols, and networks); the needs of the system users (both for organizational and individual messaging); and the systems' purposes, schedules, and requirements.

b) Compare the systems/programs: identify differences, similarities, and capabilities of both programs, both technically and programmatically.

c) Identify the differences and/or technical and programmatic features that may cause difficulty for GCCS managers, users, developers, and integrators.

d) Annotate anything that appeared to have a problem potential and present recommended actions (wherever possible) that could be taken to mitigate them. Detailed technical solutions are outside the scope of this study.

1.4 Document Organization

This report contains four sections and two appendices. Section 1.0 gives the purpose, scope, and methodology of the study. Section 2.0 provides information about the DMS program, especially as it pertains to areas of coincidence with aspects of the GCCS. Section 3.0 is a very brief view of GCCS messaging, limited to those features that are most likely to be affected by DMS. Section 4.0, "Findings, Observations, and Recommendations," contains just that: the items, technical and programmatic, that were noted during the course of the study as having the potential for causing problems, and some suggestions as to what might be done to avoid those problems.

2.0 THE DMS PROGRAM

The DMS Program Office has defined the DMS baseline as consisting of the AUTODIN and DoD e-mail on the Internet as it existed in September 1989; clearly a disjointed, resource intensive, outdated set of equipment and standards. The following paragraphs provide information on action being taken by the DMS PMO to literally "move DoD messaging technology into the 21st century." The DMS objective environment will not be realized until the year 2000 time frame but, as described below, massive changes will occur in the interim. The DMS infrastructure can be considered to consist of two major pieces: the Message Handling Environment, and the Directory Services, but for a total program perspective, the implementation strategy, security, user support, and service management shall also be considered. This section provides information about the entire DMS program with the focus directed toward the DMS infrastructure.

2.1 Background

In October 1992, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence issued an e-mail policy mandating the transition to, and use of, DMS-compliant messaging systems. Eight months later the Chairman of the Joint Chiefs of Staff Instruction, CJCSI 6211.02 dated 23 June 1993, Defense Information System Network (DISN) and Connected Systems, was issued, strengthening and clarifying the original objective: to achieve a single DoD worldwide common user IP router network. CJCSI 6211.02 directs all DoD Service/Agencies to use the "DISN as the primary wide-area network for all DoD long-haul common-user telecommunications services." In March 1995, additional implementation guidance was issued, stating that there would be one, seamless, end-to-end global electronic messaging service within the DoD, provided by the DMS. The guidance also imposed a moratorium on the acquisition of non-DMS compliant electronic messaging systems without a clear transition path to full compliance.

The United States Air Force (USAF) Acquisition Program Management Office handled source selection for the DMS contract, recently awarded to Loral, for the acquisition of DMS-compliant messaging components for implementation throughout DoD in accordance with the DMS target architecture. This initial acquisition is the first source of DMS-compliant components. Other sources will become available through future Government commodity contracts. In accordance with the transition policy guidance reflected in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI 5721.01, 28 June 1993), transition and implementation planning is underway by all the Services and Agencies (S/As).

Products delivered through these contracts will be submitted to the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) for Compliance Testing and Evaluation (CT&E). After completion of CT&E and an Operational Test Readiness Review, the DMS Initial Operational Capability (IOC) will be declared, signaling the start of the Initial Operational Test and Evaluation (IOT&E). The IOT&E will be conducted at a limited number of sites, and is currently scheduled to begin at DMS Columbus, OH in July 1996. During this period, additional, limited-rate deployment fielding will also take place. Full-rate deployment will occur after completion of IOT&E, and completion and review of Major Acquisition Information Systems Review Council (MAISRC) Milestone III requirements.

Once the initial product line offered on the DMS contract is in testing, products from other sources may be submitted to JITC for similar compliance testing. This will be done under the sponsorship of the S/A DMS Manager for which the products are required. After determination of DMS compliance, these products may be

acquired through other acquisition means and, after attaining the appropriate approval, integrated into DMS. Approval is granted based upon the ability of the new components to meet overall DoD messaging requirements. Components that negatively impact the performance, management, or security of the overall system may not be given the approval necessary to connect. At the present time the test plans and procedures are still being refined. For this reason, products other than those from the initial DMS contract will not be permitted to enter any phase of testing until the initial contract items have completed that phase.

2.2 Message Handling

The DMS target architecture and objective system represents DMS as envisioned for the year 2000 time frame. It will serve users while at home-base, traveling, or tactically deployed. Traveling users may dial in to DMS through authenticated DISN access points. Deployed users will interface to the same messaging system as those in garrison.

DMS is based on internationally developed messaging, directory, and management standards and recommendations. The implementation of International Telecommunications Union - Telecommunications Standardization Sector (ITU-T) X.400 Message Handling System recommendations to meet military messaging requirements has been defined in the Allied Communications Publication 123 (ACP-123) and its accompanying US Supplement. The use of ACP-123 by the DoD has been approved by the Military Communications Electronics Board and will be used by the United States and its Allies in the exchange of organizational messages. The US Supplement to ACP-123 also contains procedures for individual messaging.

An X.400 message is analogous to a letter sent through the postal system. The content of the message represents the letter, while the submission/delivery or message transfer envelope corresponds to the paper envelope used by the letter writer. The envelope contains all header information requested by the user. This information includes originator and recipient address, precedence, reply request, alternate delivery addresses, message type, distribution codes, etc. Some of this information is mandatory for inclusion, some is optional. ACP-123 contains all of the procedural and protocol requirements for the inclusion and use of these data elements. The content may include any number of "body parts," which are similar to attachments in e-mail packages. These body parts may contain any type of information—text, binary, or formatted documents. Files generated by multimedia applications can also be carried as an X.400 body part.

There are two types of envelopes used in X.400. The submission/delivery envelope is used for message exchange between the User Agent (UA) and its associated Message Transfer Agent (MTA), and the message transfer envelope is used in the store-and-forward process as the message moves from MTA to MTA. These envelopes contain that information necessary for the Message Transfer System (MTS) to move the message from originator to recipient. The content is not seen by the MTS.

The MTS is the heart of the model. It and consists of interconnected MTAs. The larger Message Handling System (MHS) includes the MTS, and adds UAs and Message Stores (MSs). When the actual users and Access Units (or gateways as they are commonly called), are added to the model in areas that require access from other systems, the Message Handling Environment (MHE) is complete. The Multi-Function Interpreter (MFI) is a specialized form of gateway/Access Unit and is essential to the DMS ability to interact with any other system. The Mail List Agent (MLA) is a special product designed to provide mail list expansion. It is actually a modified UA tasked with additional functionality.

Figure 2-1 depicts a notional representation of the DMS functions and components. Immediately following this figure is a set of brief descriptions of the components. The DMS UA, Directory User Agent (DUA), MS, and local directory cache can be implemented in existing personal computers or workstations, or in client-server combination with existing Local Area Network (LAN) servers. DMS users will interconnect over local area networks and/or the DISN to the DMS infrastructure message handling and directory system components. These infrastructure components will be purchased, installed, managed and maintained by DISA.

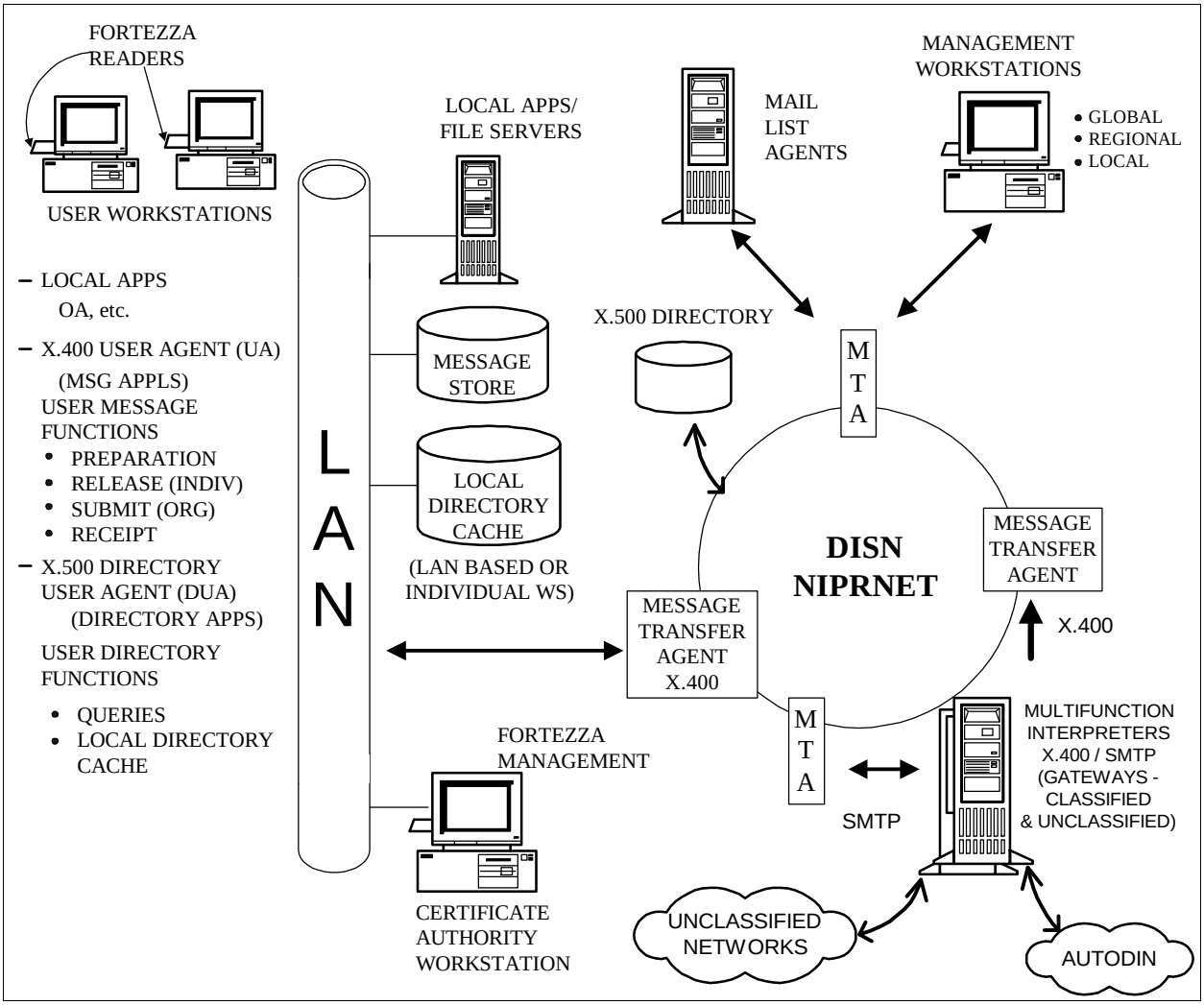

Figure 2-1. DMS Functions and Components

The DMS infrastructure contains the following components: for messaging, the DMS-UA, MS, MTA, Profiling User Agent (PUA), MLA, and the MFI. Directory services are provided by the DMS Directory System Agent (DSA), the DUA, the Administrative Directory User Agent (ADUA), and for security, the Certification Authority Workstation (CAW).

User Agent (UA): The UA is a DMS-specific implementation of the ACP-123 Military Messaging UA. The US Supplement (to ACP-123) specifies that a standardized Application Program Interface (API) be implemented to allow different messaging-enabled applications (e.g., Electronic Data Interchange and Records Management) to access DMS services.

Profiling User Agent (PUA). The PUA is a special type of UA configured to automatically perform onward distribution of received organizational messages based on preregistered message characteristics.

Mail List Agent (MLA): The MLA is a specialized device that expands a Mail List (ML) on behalf of a user. A user composes a message with the name of the ML and forwards it to that of the MLA. The MLA then expands the address field of the message to that of the ML member, including the necessary processing to maintain writer-to-reader security.

Multi-Function Interpreter (MFI): The MFI's chief function is translation of messages between ACP-123 protocols and other non-DMS message systems (e.g., ACP-127, Simple Mail Transfer Protocol/Multipurpose Internet Mail Extensions [SMTP/MIME]). The MFI provides a means to maintain interoperability with existing systems while ensuring communications with non-DoD entities, such as the commercial sector.

Directory User Agent (DUA) and Directory System Agent (DSA). The DUA is an application layer process that represents a user in accessing the Directory. DUAs interact with the Directory by communicating with the DSA, which is another application layer process. DSAs collectively retain a physically distributed, but logically centralized, data store. The DSAs cooperate to provide the overall directory service. By design, virtually any DUA can access virtually any DSA. DUAs also provide features to: 1) assist users in composing queries and interpreting responses, 2) provide security services, and 3) locally cache directory information. In the DMS architecture, any component requiring X.500 Directory service can implement a DUA. The most common implementation of the DUA will be in conjunction with the DMS UAs. The UA requires information from the X.500 Directory in order to address messages. The DUA obtains this information from the X.500 Directory and supplies it to the UA in support of message preparation.

Administrative Directory User Agent (ADUA): ADUAs are DUAs enhanced to provide directory administrators the ability to modify X.500 Directory entries. The Update Authorities use the ADUA in combination with the Update Authority Components and/or Message Preparation Directory applications to manage, modify, add, and delete X.400, SMTP, and AUTODIN information contained in the DMS X.500 Directory. ADUA applications will reside on the CAW to perform distributed directory and security management tasks. The ADUA, integrated with the Management Work Station (MWS) will manage the Directory and analyze the Directory's performance.

Certificate Authority Workstation (CAW). The CAW is the source of certificate and key management. It is the tool used by the Certificate Authority to perform FORTEZZA card creation and

management functions, create X.509 certificates and post them to the X.500 Directory, post Certificate Revocation Lists, and distribute Compromised Key Lists. The CAW software is operated on a trusted platform with two FORTEZZA readers, one for the Certificate Authority's card and the other for the user's card being programmed. Along with the CAW software, a local database is maintained for all future reference of personalities and certificates. Additional information regarding users may also be included in this database.

The user will select the DMS messaging application from a menu or Graphical User Interface (GUI) presented by their office automation system. (In the case of the GCCS, this is a new feature that will have to be provided in the COE). The DMS UA software provides the message functions for both organizational and individual messaging. These functions include preparation, submission, transmission, and reception, as well as organizational message release and distribution determination. The DMS user has access to a local directory cache containing the addresses, security certificates, and capabilities of all the recipients with which the user communicates on a regular basis. When desired information is not present in the local directory cache, queries are formulated by the DUA software, and sent to the DSA serving that user. The global DoD directory will comprise a number of interconnected DSAs.

The MS provides the user with a "mail box" where messages are delivered when the user is not available. These services are accessed from the UA and allow users to properly handle delivered messages. The message store accepts delivery of messages on the user's behalf, and holds them until accessed by the user. This component also submits messages on the user's behalf to the appropriate submission/delivery point in the MTS. A significant feature of the MS is the stored message alert service. This service will alert users, when connected to their MS, of the arrival of high-precedence messages. If the user is not connected, then the user can instruct the MS to autoforward the message to an alternate delivery address or site, according to local policies, that can receive and act on these messages.

Users are connected to the DMS infrastructure for submission and receipt of messages and to obtain directory and management services. The DMS infrastructure components include the MTS, consisting of a hierarchically connected set of MTAs, distributed DSAs, MLAs, and MFIs. Messages are submitted to, or delivered from the MTA serving a particular user. They also perform store and forward message transfer services to efficiently move message traffic from writer to reader. DSAs contain the distributed directory information and information from the global DoD Directory Service. MLAs ensure that messages addressed to single collective addresses, called "mail lists," are delivered to the multiple addresses that are part of that collective. MFIs provide protocol translation for interoperability with legacy systems during the transition, and with non-DMS compliant systems external to the DoD after achievement of the objective system.

2.3 Directory Services

There are a number of different directories in use today. This is a problem that the DMS Directory Service will correct. Organizational messaging directories supporting AUTODIN, such as the General Service directories, which include the Message Address Directory (MAD) and ACP-117, and the intelligence community's DSSCS Operating Instruction (DOI) 102, provide plain language addresses, and routing information as needed. Because of the size and the distribution requirements of these paper directories, they encounter information currency problems as well as untimely distribution schedules.

E-mail plays an important role in individual messaging. While e-mail does use automated directories, the directories are designed for the LANs, and provide directory information for a particular e-mail package such as Microsoft Mail, CC:mail, Novell, Banyan, or any other proprietary e-mail package. These directories are each centrally managed for their own, individual, e-mail packages. They are disjoint and frequently do not interoperate with other vendors' e-mail packages. Since the directories are not tightly managed, they do not provide accurate addressing information, often requiring the user to use the phone to get the e-mail address needed for a message.

The DMS X.500 Directory Service is an automated service developed from the internationally-accepted ITU-T X.500 Standard, with the objective of providing a distributed directory service based on a common agreement for implementation. The directory service supports both organizational and individual messaging utilizing the DMS-wide directory schema. This schema provides the format for the structure and contents of the directory, as well as the rules for its use. The directory entries contain messaging information such as user names and addresses, organizational names/addresses/roles, distribution lists, security information, and user capabilities. The directory service will evolve to the Department of Defense (DoD) Directory supporting non-messaging X.500 directory entries such as postal addresses, telephone numbers, facsimile numbers, etc. The directory service also provides access controls permitting particular users to get specific information.

The directory service provides the mapping of a name to an address, facilitating the communications process. Computers and application software also use directory services to access presentation addresses and host addresses. When composing a message, a user needs to be able to address the message to a recipient. After registering and obtaining a FORTEZZA card, the user can access the Directory Service through the DUA and obtain that addressing information. If the user wants to store this information locally at his DUA, he or she can. Local storage provides the user with the ability to keep frequently used addressing information readily available; however the user has the responsibility of ensuring the accuracy of the locally stored data. There is the risk that the information in the directory could change and the user may not be aware of the change.

The ITU-T X.500 Recommendation on Directory Services defines the functions and protocols necessary to ensure that directory systems developed independently can interoperate. The DMS PMO is leading an Allied military effort to develop ACP-133, "Implementation Guidance for Directory Services." This document will guide the interaction, schema, and user information implemented in X.500 directories within the Allied military community.

As depicted in Figure 2-2, the directory infrastructure, specifically regional DSAs, will support requests from their associated users. Further queries can be made from DSA to DSA by either chained or multi-chained interactions, or by sending a referral back to the user for a follow-up query to a distant DSA.

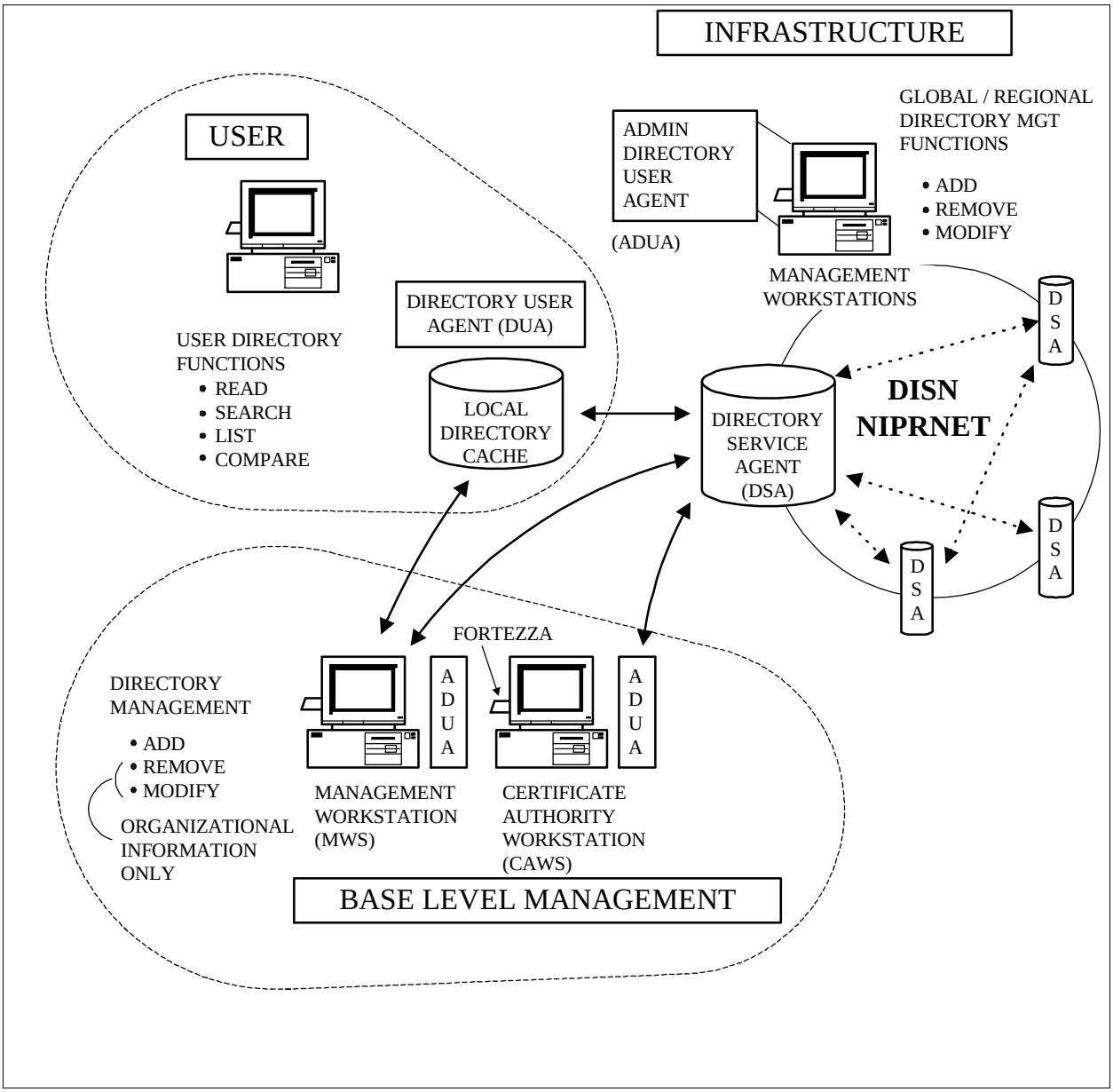

Figure 2-2. DMS X.500 Directory Services

2.4 DMS Security

For DoD to accomplish its warfighting and peacekeeping missions, the various DoD systems that comprise the Defense Information Infrastructure (DII) must establish connections with non-DoD systems. These connections include those to our trading partners, academia, DoD contractors, other U.S. Government Agencies, and our allies and military coalition partners. While these connections are essential to accomplishing DoD's mission, they are also make DoD systems vulnerable to active and passive attacks from foreign intelligence agencies, network hackers, and the computer virus infections that plague communications and information systems

throughout the world. These threats are in addition to those posed by insiders willing to compromise DoD systems security.

DII security will use a common set of security products, a common Electronic Key Management System, and a common directory system. However, the commonality between the security solutions developed for the various DoD programs goes considerably farther. The DMS will be the first major deployment of Multilevel Information Systems Security Initative (MISSI) products. The security infrastructure and security products deployed to support the DMS will also be used to secure other DoD applications.

The current messaging environment can be characterized as system-high islands of proprietary e-mail systems that communicate via SMTP mail through proprietary mail gateways. There are no systems that meet validated DMS requirements. This is especially true of the security requirements. There is no writer-to-reader security for confidentiality, integrity, or non-repudiation. Also, while there may be some local access control, identification & authentication, and audit services, these are generally rudimentary, non-standard services.

The MISSI program is a National Security Agency (NSA) effort to develop and field security products to address these issues. The program takes an evolutionary, building-block approach, starting with the development and fielding of products to protect the exchange of Sensitive But Unclassified (SBU) information. Additional products and capabilities are under development to protect classified information up to the Secret level. Eventually, products that are capable of protecting the exchange of all levels of information from SBU through Top Secret/Sensitive Compartmented Information (TS/SCI) will be developed and deployed.

Two of the initial MISSI products, the FORTEZZA cryptographic card and the CAW, will be used to protect the initial DMS infrastructure and begin protecting the SBU organizational and individual messaging. Security for SBU messaging during the DMS IOC is provided on a per-message basis by the FORTEZZA card. This Personal Computer Memory Card Interface Association Type II card contains the algorithms in firmware and private key certificates in static random access memory (RAM) used to electronically sign, hash (provide integrity checks), and encrypt messages. This mechanism is also used to apply authentication services to directory queries. The CAW is used to program and update the FORTEZZA cryptographic card. Additionally, the CAW is used to provide updates to the X.500 Directory.

This initial security capability will support the downsizing of AUTODIN. Later MISSI products, including the FORTEZZA+ cryptographic card, an upgraded CAW, business-grade firewalls, and high-assurance automated guards such as the Secure Network Server, will provide improved security and make it possible to phase out, and eventual close, AUTODIN. Ultimately, MISSI products, such as a high-assurance operating system and a communications software security package, will be available to support the complete range of DoD and Intelligence Community information exchange.

2.5 DMS Acquisition and Implementation Strategies

The DMS Program is employing an innovative acquisition strategy designed to influence development of commercial-off-the-shelf (COTS) products while maintaining maximum competition and acquisition flexibility. Vendors are encouraged to provide COTS solutions to meet DoD's messaging, directory service, security, and service management requirements. Establishment of a separate, DMS-compliant testing environment will ensure these products satisfy DMS functional, security, performance, conformance, and interoperability requirements. More significantly, this testing environment will allow any vendor who did not bid, or was not

involved in the award of the primary DMS acquisition contract, to submit products for DMS compliancy certification. Once certified, these products will be available for purchase by the S/As from a certified products list. This acquisition strategy will provide DoD and other designated Federal agencies maximum acquisition flexibility and cost savings resulting from competition and large-quantity purchases.

The DMS primary acquisition contract is an indefinite delivery/indefinite quantity acquisition of DMS-compliant products and services. This allows the Services, Agencies, and DISA to procure those products and services each deems necessary to achieve the target DMS architecture. DISA will procure hardware and software products and support services necessary to engineer, integrate, plan, deploy, implement, and maintain/manage the DMS infrastructure. Users will procure software and services necessary to integrate, implement, maintain, and manage their user components. Following compliance test and evaluation of the initial system, IOC is tentatively scheduled for early 1996. At this time, IOT&E and limited-rate deployments will commence.

As described in the November 1994 DMS Target Architecture and Implementation Strategy (TAIS), the evolutionary transition from the DMS Baseline to the target architecture is characterized by the transition of baseline systems, achievement of target architecture capabilities, and associated milestones. It enables near-term base level cost and manpower reductions by the early introduction of DMS transitional components developed in coordination with, and shared among, the S/As. The strategy provides for the evolutionary development and implementation of DMS policies, procedures, protocols, services, and components, which rationalize the programmed progression to the target architecture. Additionally, it includes operational testing of new components, protocols, and procedures in live-user environments to provide proof of purported benefits prior to widespread deployment.

The DMS Implementation Strategy was jointly developed by the Services and Agencies represented on the DMS Implementation Planning Working Group (IPWG). The IPWG is supported by several sub-working groups and action teams tasked to address particular issues. There is also support from the DISA matrix structure to address such things as engineering the system infrastructure and modeling performance. At the highest level, planning included all participants and considered all aspects of the fielding process regardless of S/A affiliation. This planning will be tailored to individual S/A fielding requirements and used for S/A planning. As Fielding Conferences occur, planning will be tailored by the S/A to consider requirements at each designated site.

There are at least three program-wide tasks of sufficient criticality to warrant discussion here. These are the transition of AUTODIN, achieving DMS-Compliant X.400 messaging and X.500 Directory Services, and achieving DMS Final Operating Capability (FOC).

- **Transition of AUTODIN:** The initial transition emphasizes automation of existing Telecommunications Center (TCC) functions and extension of messaging services to users to reduce cost and staffing at the base level. Simultaneous deployment of regional transition components during this phase provides AUTODIN directory improvements, an AUTODIN-to-DDN interface capability, and consolidation of AMHSs. These efforts are currently in progress and are allowing the S/As to phase out resource-intensive base-level TCCs, to migrate AUTODIN data pattern message traffic to the DISN, to begin the organizational messaging transition, and to posture the organizational and individual messaging communities for evolution to DMS-compliant messaging.

- **Achieving DMS-Compliant X.400 Messaging and X.500 Directory Services:** IOC for X.400/X.500 individual and organizational messaging with Message Security Protocol (MSP) protection will be achieved through deployment of DMS-compliant components acquired through the DMS primary acquisition contract. This achievement will produce the most obvious architectural changes and improvements for the users with deployment of an integrated DMS, based on X.400 messaging (rather than distinct AUTODIN and proprietary e-mail) and X.500 directory services. As TCC functions and responsibilities are shifted to DMS UA workstation applications, TCC phase-outs will be accelerated. With the simultaneous deployment of X.400 MTAs, X.500 directory services, DMS service management capabilities, and MISSI security protection mechanisms, an integrated X.400/X.500/MSP DMS organizational and individual messaging system will be in place and maturing.

- **Achievement of DMS Final Operating Capability (FOC):** In March 1994, the DMS program became subject to MAISRC oversight. Prior to this, management oversight was provided by the OSD/C3I Defense Acquisition Board (DAB), C3I Systems Committee and the ASD/C3I Chaired DMS Panel. Development, coordination, and approval of all DMS-related activities were in accordance with the guidance provided by these oversight boards/panels. Full rate deployment will commence following Milestone III Decision Review in late 1996. Achievement of the DMS FOC enables the closure of the last Automatic Switching Center (ASC). The X.400 / X.500 / MSP organizational and individual messaging system will mature, and the target architecture will be achieved. Remaining TCCs will be closed, and transitional components deployed earlier will be phased out. Although evolution of the local and long-haul backbone networks is not part of the DMS Program, achieving the DMS target architecture relies upon the availability of mature DII network capabilities.

2.6 Requirements

The DMS Program was established in response to Joint Staff validated messaging requirements as identified in the Multicommand Required Operational Capability (MROC) 3-88 (with Change 1, August 1993), and the DMS Required Operational Messaging Characteristics (ROMC) (with Change 1, April 1994). The DoD high-level requirements for messaging, as described below, were defined in a joint service and agency forum and then documented in the MROC. The ROMC was developed to provide more specific detailed, and where possible, quantitative and qualitative requirements statements. These validated requirements establish the need for writer-to-reader messaging service that is accessible from worldwide DoD locations, tactically deployed users, and other designated Federal Government users, with interfaces to Allied users and defense contractors. The DMS is required to support the exchange of electronic messages at all classification levels, compartments, and handling instructions. In addition to maintaining high reliability and availability, the DMS must interoperate with present messaging systems as the DMS evolves from its current configuration to the target architecture. ACP-123 contains additional detailed requirements for the NATO and other Allied systems interfaces.

The top-level requirements specified in the MROC are listed below (numbering from the original is preserved). These are referred to as "Elements of Service" in the ACP series of documents.

- **Connectivity/Interoperability:**

  (1) The DMS should allow a user to communicate with any other user within the DMS community. The community of users includes organizations and personnel of the DoD to include deployed tactical users. In addition, the DMS must support interfaces to systems of other government agencies, and defense contractors. System users may be fixed, mobile, or transportable.

  (2) Connectivity must extend from writer to reader. Messages should be composed, accepted for delivery, and delivered as close to the user as is practical. Current efforts, such as extension of automation to users and improved base level message distribution systems, are responsive to this requirement.

  (3) The DMS will operate over tactical data distribution systems. The DMS must be interoperable with and provide standard interfaces for allied systems. It should lead DoD's migration to international standards and protocols.

- **Guaranteed Delivery/Accountability:**

  (1) The DMS must, with a high degree of certainty, deliver a message to the intended recipient(s). If the system cannot deliver a message, a method of promptly notifying the sender of the nondelivery must be available.

  (2) For organizational message traffic, the DMS must have the capability to maintain writer-to-reader message accountability.

- **Timely Delivery:** The DMS must recognize messages that require preferential handling. The urgency of the most critical information requires handling above and beyond simple priority. The DMS must dynamically adjust to changing traffic loads and conditions to provide timely delivery of critical information during peacetime, crisis, and war. Delivery time for a given message will be a function of message precedence and system stress level.

- **Confidentiality/Security:** Confidentiality precludes access to or release of information to unauthorized recipients. The DMS must process and protect all unclassified, classified, and other sensitive message traffic at all levels and compartments. The DMS must maintain separation of messages within user communities to satisfy confidentiality. Security is based upon requirements for integrity and authentication as well as confidentiality.

- **Sender Authentication:** The DMS must unambiguously verify that information marked as having originated at a given source did in fact originate there. For organizational traffic, a message must be approved by competent authority before transmission.

- **Integrity:** Information received must be the same as information sent. If authorized by the writer, the DMS may make minimal format changes to accommodate differences in capabilities between the

component systems serving the writer and the reader. However, the DMS must ensure that information content of a message is not changed.

- **Survivability:** The DMS must provide a service as survivable as the users it serves. It must not degrade the survivability of systems interfaced to it. Methods such as redundancy, proliferation of system assets, and distributed processing may be employed. Surviving segments of DMS must be capable of reconstitution.

- **Availability/Reliability:** The DMS must provide users with message service on an essentially continuous basis. The required availability of the DMS should be achieved by a combination of highly reliable and readily maintainable components, thoroughly tested software, and necessary operational procedures.

- **Ease of Use:** The DMS must be flexible and responsive enough to allow user operation without extensive training. Use of the DMS should not require the knowledge of a communications specialist.

- **Identification of Recipients:** The sender must be able to unambiguously identify to the DMS the intended recipient organizations or individuals. The necessary directories and their authenticity are part of the DMS.

- **Message Preparation Support:** The DMS must support user-friendly preparation of messages for transmission, to include services such as U.S. Message Text Format (USMTF) assistance.

- **Storage and Retrieval Support:** The DMS must support storing messages after delivery to allow retrieval for such purposes as readdressal, retransmission, and automated message handling functions such as archiving and analysis, with the capability of incorporating segments into future messages. The minimum storage period for organizational messages will be specified by Allied Communications Procedures.

- **Distribution Determination and Delivery:**

  (1) For organizational message traffic, the DMS must determine the destination(s) of each message (in addition to the addressee(s) specified by the originator) and effect delivery in accordance with the requirements of the recipient organization.

  (2) For individual message traffic, the DMS must effect delivery of each message to the individual(s) specified by the originator.

3.0 GCCS MESSAGING

3.1 Organizational Messaging

The AUTODIN organizational messaging capability for the GCCS is provided by the Automated Message Handling System (AMHS) developed by the Jet Propulsion Laboratories (JPL). Operating in the secret-high security mode, the JPL AMHS is a DMS Component Approval Process (CAP) approved AMHS for at least two locations, US Transportation Command, (USTRANSCOM) and European Command (EUCOM). Inbound AUTODIN message processing includes automated message receipt, distribution, search, and retrieval while outbound message processing includes message generation, coordination, and release.

Three primary components comprise the AMHS. These components are the Standard Automated Terminal (SAT), an AMHS Server and software, and AMHS client software. An additional component that affects AMHS operations, although not a part of the AMHS *per se*, is the Network Information Service (NIS+) server. The NIS+ server provides an administrative functionality for general GCCS operations support, including part of the security functionality for the AMHS.

The SAT provides access to AUTODIN via a back-side interface to an Automated Multi-Media Exchange (AMME), Air Force/Automated Message Processing Exchange (AF/AMPE), Communications Support Processor (CSP), Pentagon Telecommunications System (PTC), Message Distribution Terminal (MDT), or Local Digital Message Exchange (LDMX). The SAT performs all necessary processing for receipt and transmission of AUTODIN messages.

The AMHS Server hosts the client/server applications, the Verity TOPIC Real-Time applications and database, and the SAT applications. Inbound messages from the SAT are processed by the Server and stored in the TOPIC Real-Time database. The TOPIC Real-Time software application profiles the inbound message for distribution determination based on established user profiles.

The AMHS client software resides on the user workstations and provides the user interface to the AMHS. Message review, retrospective search of the database, message creation and coordination, and outbound message processing capabilities are also provided.

A LAN segment can be used for a networking environment that supports Transmission Control Protocol/Internet Protocol (TCP/IP) intercommunications among the components that comprise the AMHS.

Alternatively, the AMHS SAT and server can reside on the GCCS LAN. The AMHS server software may also be installed on the GCCS server if a separate AMHS server is not needed by the traffic volume at a particular site.

The GCCS currently operates in the secret, system-high security mode. Wide Area Network (WAN) connectivity in support of GCCS applications and individual messaging is via the Secret Internet Protocol Network (SIPRNET). Organizational messaging is provided by the AMHS over AUTODIN. This message traffic can be originated at less than the system-high classification level. However, messages must be reviewed by a Message Release Authority (MRA) for correct labeling prior to submission to the SAT for processing and submission to AUTODIN.

3.2 Individual Messaging

The GCCS COE provides a wide range of individual messaging capabilities over and above basic e-mail. These are described in the following paragraphs.

3.2.1 Internet Relay Chat

Internet Relay Chat (IRC) is a program that allows multiple users to participate in on-line conferences in the form of near real time text inputs from the individual to the group. It is implemented as a network of IRC servers. Users interact with IRC via IRC clients. A user invokes an IRC client and directs the client to connect to a server. Once connected, the user participates in conferences/conversations by joining specific channels. By joining a channel, the user will then receive all messages sent to that channel. Further, when the user inputs a message to the channel, the message is forwarded to all other clients on the same channel (including clients attached to other servers in the network).

The IRC server is *ircd*. It is a UNIX daemon that runs continuously on a server platform. Each server location will have at least one IRC server running at all times. *Ircd* is written in C, and utilizes sockets for interprocess communication (IPC). The default is port 6667.

IRC is non-persistent in that messages are not saved. It is very interactive. When a user types something on his screen, it is very quickly transmitted to all other users currently connected to that conference. However, when a message is sent while a user is not connected, that user will not be able to see that message. Features supported include private channels (users not on the channel cannot see who is on the channel), secret channels (users not on the channel cannot detect that the channel exists), keyed channels (users must know a password to join the channel), invitation-only channels (a channel operator must send a user an invitation before the user can join the channel), and moderated channels (channel operators can provide/remove permission to individuals to input messages to the conference).

The GCCS COE is providing Zircon, an X-based package that provides an elegant GUI interface to IRC. It is written in the Tcl scripting language, and thus requires that Tcl, Tk and Tcl-dp be present on the machine from which it is executed. Features include side-bar conversations (two-way conversations invisible to others), pop-up channel displays (iconified channel windows will restore themselves when a message arrives on the channel), and queries regarding the identity of other users.

3.2.2 Internet News

Internet News (referred to simply as News) is a bulletin-board-style broadcasting service. Articles are uploaded to the server network, which distributes the article to all sites. Users subsequently connecting to a server can then view the article, up to the point at which the article expires (and is then purged from the server[s]). News is organized into newsgroups, according to topics of interest. On the Internet, newsgroups are organized into a hierarchy to allow users to locate newsgroups of interest. For example, <rec.pets.dogs> is a newsgroup discussing dogs. It is under the recreation category, and further under pets. A user that knows about the existance of <rec.pets.dogs> would (correctly) deduce the existence of <rec.pets.cats>. Each article posted to News is associated with one or more groups. Users subscribe to only those newsgroups that are of interest to them, and thus are not forced to search through unwanted articles.

News is designed as a network of servers to which clients attach. The GCCS COE is providing *inn* (Internet News) as the server. This program is written in C, and also utilizes sockets for IPC. Its port is 119. This server is highly configurable.

Two client software packages are being provided: *xrn* and *tin*. Both are written in C. Features supported by these products include the ability to subscribe/unsubscribe to newsgroups, read articles, follow a thread (a series of articles in a newsgroup which have the same subject line), upload and download files, and send e-mail to article authors.

3.2.3 World Wide Web

The World Wide Web (WWW) operates on an entirely different principle than do IRC or News. IRC and News are "active" services, servers that transmit information to the client/user who selects what they will/will not receive. The Web, on the other hand, is a passive information supplier. The Web user directs their browser software to connect to specific Web servers to retrieve documents of interest. These documents may have within them embedded links to other Web documents; a user can click on a link to automatically download the document it points to.

Thus, the architecture of the Web is different from that of IRC or News. Instead of having the servers communicate with each other and the clients via a single (local) server, WWW servers are autonomous; i.e., clients must directly access the server that has the information that the client wants. There are other differences as well. IRC and News are primarily text-based applications. It is possible to post binary files to News, but only by "uuencoding" them (encoding the binary as a text file). The Web, on the other hand, supports protocols that in turn support the transmission of binary data (including http and ftp).

Two WWW server packages are being provided for GCCS. Netsite is a commercially available WWW server produced by Netscape Communications Corporation. Httpd is a public-domain server available from the National Center for Supercomputing Applications (NCSA). Both support restricting user access to documents based either upon userID+password or upon the location of the user (machine connecting from).

The browser software for GCCS is Netscape (also produced by Netscape Communications) (some sites have installed Mosaic, but this is not being supplied as a segment). Netscape can display files in a wide variety of formats, including html (hyper-text markup language—the workhorse of the Web), text and gif (graphics). It also has the ability to execute other programs for displaying files that are in other formats (such as postscript, jpeg, mpeg, wav, etc.).

4.0 FINDINGS, OBSERVATIONS, AND RECOMMENDATIONS

This section contains short discussions of aspects of DMS/GCCS messaging implementation that appear to have the potential for causing problems for the GCCS engineers. Recommendations are offered wherever possible, but detailed technical solutions are not within the scope of this paper. The findings or observations that follow in Subsection 4.1 are generally grouped by functional area, such as Security, Messaging, or Directory Services. Following the description of each potential problem are questions that need to be answered to help avoid those problems. General recommendations for both near-term and long-range actions are then provided in Subsection 4.2.

4.1 Findings and Observations

4.1.1 DMS Architecture

DMS is heavily focused on UAs. This, together with the fact that DMS is an Application Layer program, means that UAs with well-defined APIs must be made available. APIs are normally required between functional applications and the messaging system. Presently, the DMS Program is still in the process of developing a standardized specification for APIs that can be applied towards these kinds of requirements.

- Questions:
  - When will these APIs be available?
  - Are there preliminary versions that the GCCS engineers can use to begin evaluation?

The MFI is going to be an essential fixture during the transition period, and there is some concern expressed in the documents researched during this study regarding how it will handle attachments when converting from SMTP mail. If an attachment is a simple text message then no problem is foreseen. But, if an attachment is a binary attachment, then problems are presented. In handling this through the MFI, a binary attachment would be converted to a MIME attachment. Initially, Version 1.0 of the baseline DMS product will be built around a simplistic RFC 1521 MIME attachment. While this is not a robust capability, it is the initial point for beginning to build future releases and greater MIME capability. The main problem that DMS is confronting is the multiple MIME RFCs that exist today.

- Questions:
  - Is there a minimum set of attachment types that are known to work?
  - If so, are these used by GCCS?
  - Is there a set of attachment types that are known to cause problems?
  - Can/should GCCS avoid these?

4.1.2 Security Issues

The FORTEZZA card is a crypto peripheral (although FORTEZZA cards are not COMSEC accountable) that performs Government-grade encryption. U.S. law prohibits export of cryptography. How will users take their FORTEZZA cards abroad? The stories of notebook computers being confiscated at airports for having Norton Utilities and other commercial products with encryption capabilities seem to indicate a cause for concern.

- Questions:
  - For forces deploying as units this will not be a problem, but what about individual travel?
  - Is the only solution to have a new FORTEZZA card prepared at the destination?

Text of e-mail messages will be signed and encrypted, and DMS UAs will sign and encrypt all attachments as well. Attachments are an integral part of the X.400 message, unlike SMTP where the message and attachments are separate. The next question is: What happens when a user needs to send a message to a person who does not have qualifications to receive, i.e., cannot receive Secret, or is not a DMS subscriber? The current answer is that the security checks will fail and the user will not be allowed to send the message. It seems clear that two distinct individual messaging systems will be in use for a long time. As discussed earlier, the GCCS community will not be affected any time in the near future, by virtue of the different networks used (GCCS on the SIPRNET and DMS on the Not Classified but Sensitive Internet Protocol Pointer Network [NIPRNET]). GCCS users will continue to use the individual messaging capabilities of the GCCS COE within that community.

- Questions:
  - Is individual messaging outside the GCCS community within the scope of the GCCS program?

  - If so, should the GCCS COE be modified to accommodate X.400 and X.500, or should a separate, DMS-compliant capability be provided? Clearly, the intent of DMS is standardization.

There is a DMS requirement to protect NIPRNET from Internet. All Services/Agencies are now buying and installing "firewalls." Applications gateway-type firewalls that successfully pass the DMS compliance process will be included on the DMS-compliant products list. According to the DMS literature "Packet filter-type Firewalls that are properly configured should not interfere with the DMS applications processes." The concern for the GCCS engineering community must be that any applications gateway-type firewalls in use by GCCS must support DMS messaging, directory, and management services. DMS documentation researched for this study contained no requirements or specification information for DMS-compliant firewalls. At least part of the solution may be that the local Designated Approval Authority may decide which firewalls are required to protect "other" communications assets such as IP routers, file servers, print servers, etc.

- Questions:
  - Do these standards exist yet?
  - Are they available to the GCCS engineers?
  - How much risk are we incurring by installing firewalls without knowing the DMS standards?

According to DMS documentation, DMS is to replace AUTODIN. AUTODIN cannot terminate until DMS supports TS/SCI. DMS will support SCI messaging across the Joint Worldwide Intelligence Communications System (JWICS) beginning in 1996. The integration of the DMS infrastructure on the NIPRNET and the DMS infrastructure on JWICS will be accomplished when security products that can support such integration are available for deployment. In the meantime, the DMS is working with NSA to develop an X.400 guard that allows NIPRNET/SIPRNET connectivity. The target date for this product is October, 1996.

- Questions:
  - What needs to be done to eliminate the redundancies that will occur with a NIPRNET-to-X.400 guard for MFI-to-AMHS set of connections?

  - How can those redundancies be eliminated without losing essential AMHS functionality, such as retrospective search?.

The MISSI audit manager is an NSA project that is to provide agents (to run on managed components) and a manager (remote from the components). Together, these perform security audit generation and analysis functions. There are similar capabilities, which were requirements for the MWS, a central control point for network control, management, and audit. As such, there is a degree of redundancy between these two efforts, which is the result of the timing of the two acquisitions. The DMS program (through DISA, Loral, and the USAF) is working with the MISSI audit manager team (through NSA) to determine the best approach to performing security management functions, with a goal of performing the required functions without redundancy. That effort should be closely monitored, because similar redundancies with existing GCCS audit mechanisms will be almost inevitable.

- Question:
  - Has a GCCS point of contact for security audits been established and are they in touch with the appropriate DMS office?

4.1.3 Management/Programmatic Issues

There is a DMS requirement for every message (individual and organizational) to be signed and encrypted. This, in turn, requires every messaging user to have an individual FORTEZZA card. The impact on GCCS is still in the future, but planning for FORTEZZA card readers and card management procedures, personnel, and costs should be underway.

- Question:
  - What costs, tasks, etc., are the responsibility of GCCS, the S/As, DMS, NSA?

According to the DMS PMO, a requirement has not been identified for DMS to provide retrospective search capabilities. Consequently, the initial DMS PUA is limited to performance of profiling functions associated with distribution determination of received organizational messages, and the initial PUA does not perform retrospective searches that are performed by current customized AMHS profilers. That requirement should be identified so that it may be considered by the DMS Configuration Control Board (CCB) as a possible Engineering Change Proposal (ECP) to the Loral contract. Such a change would require determination if DMS is the proper programmatic vehicle for provision of full AMHS capabilities. At present the DMS PMO is not taking a position either way.

- Question:
  - What would it take for the AMHS to access the DMS MS, in addition to or instead of the AMHS message database, for retrospective searches?

4.1.4 Fielding and Implementation Issues

The new CT&E process will replace the current CAP Certification for DMS hardware and software. This new process is still being improved, and changes to the test process will be posted on the JITC Home Page. The address for the JITC Home Page is WWW at http://jitc-emh.army.mil. Non-Loral products can enter US POSIT Standards Conformance Testing at any time. However, the JITC portions of DMS Compliance T&E (DMS Standards Conformance Testing, Protocol-level Interoperability, and Functionality, Security and Performance Testing) of non-Loral products will not begin until Loral products complete the test. For example, if the Loral products in the first version of DMS have completed DMS Standards Conformance Testing, and are progressing toward the next element of test—Protocol-level Interoperability, then non-Loral products can begin DMS Standards Conformance Testing. The reason for this is that the test processes have thus far only been executed in laboratory environments during development. The actual tests of Loral products may result in changes to the methodology or the procedures developed for the test. This is important to the GCCS program because the program has products and/or suppliers that may be affected. Firewalls are one example. The entire AMHS is another, if it is ever to be used in any other than a secret, system-high environment.

- Question:
  - Can the GCCS program get a DMS expert on DMS test procedures and requirements to help with an evaluation of actions that GCCS needs to be initiating?

4.2 Recommendations

4.2.1 Near Term (at least through GCCS Rel 3.0)

- Confirm (with DMS PMO) that individual messaging as provided by the GCCS COE will be allowed to continue on the SIPRNET at least until the DMS MLS products are tested, approved and available.

- Confirm (with DMS PMO) that MFI will be available to provide x.400 wrap / unwrap for AUTODIN/AMHS/organizational messaging until AMHS modifications are through JITC test/approval process.

4.2.2 Long-Range (Post-GCCS Version 3.0)

- Initiate tasking to estimate cost, value, and feasibility of modifications to existing AMHS to accommodate X.400 envelope protocols without MFI intervention. In parallel, investigate alternatives, and particularly look at this as an opportunity to "unbundle" the AMHS reliance on specific, proprietary products (for example: the Verity TOPIC/Sybase database and query dependency, and the exclusive use Applix for MTF editing and message preparation).

- Initiate tasking to incorporate the X.500 addressing and directory schema into existing individual messaging capabilities (e-mail and teleconferencing), as these capabilities continue to evolve and improve.

- Initiate tasking to plan for the inclusion of MISSI/FORTEZZA products and standards in future GCCS releases. Plan needs to include budget, schedule, training and management issues as well as the technical considerations.

APPENDIX A

ACRONYMS AND ABBREVIATIONS

APPENDIX A: ACRONYMS AND ABBREVIATIONS

ACP	Allied Communications Publication
ADUA	Administrative Directory User Agent
AF/AMPE	Air Force/Automated Message Processing Exchange
AMHS	Automated Message Handling System
AMME	Automated Multi-Media Exchange
API	Application Program Interface
AUTODIN	Automatic Digital Network
CAP	Component Approval Process
CAW	Certification Authority Workstation
COE	Common Operating Environment
COTS	Commercial-Off-The-Shelf
CSP	Communications Support Processor
CT&E	Compliance Testing and Evaluation
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DMS	Defense Message System
DSA	Directory System Agent
DUA	Directory User Agent
FOC	Final Operational Capability
GCCS	Global Command and Control System
GDTS	GCCS DMS Transition Strategy
GUI	Graphical User Interface
IFFC	Interim FORTEZZA For CLASSIFIED
IOC	Initial Operational Capability
IOC(N)	Unclassified But Sensitive Initial Operational Capability
IOT&E	Initial Operation Test and Evaluation
IPC	Interprocess Communication
IPWG	Implementation Planning Work Group
IRC	Internet Relay Chat
ITU-T	International Telecommunications Union-Telecommunications Standardization Sector
JITC	Joint Interoperability Test Command
JPL	Jet Propulsion Laboratory
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LCC	Local Control Center
LDMX	Local Digital Message Exchange
MAISRC	Major Automated Information System Review Council
MDT	Message Distribution Terminal
MFI	Multi-Function Interpreter
MHE	Message Handling Environment
MHS	Message Handling System
MIME	Multi-Purpose Internet Mail Extensions

MISSI	Multilevel Information System Security Initiative
MLA	Mail List Agent
MRA	Message Release Authority
MROC	Multicommand Required Operational Capability
MS	Message Store
MSP	Message Security Protocol
MTA	Message Transfer Agents
MTF	Message Text Format
MTS	Message Transfer System
MWS	Management Work Station
N	Unclassified But Sensitive (Not Classified)
NCSA	National Center for Supercomputing Applications
NIPRNET	N Internet Protocol Router Network
NIS+	Network Information Service
NSA	National Security Agency
PMO	Program Management Office
PTC	Pentagon Telecommunications System
PUA	Profiling User Agent
RAM	Random Access Memory
RCC	Regional Control Center
RFC	Request for Comments
ROMC	Required Operational Messaging Characteristics
S/A	Service/Agency
SAT	Standard Automated Terminal
SBU	Sensitive But Unclassified
SIPRNET	Secret Internet Protocol Router Network
SMTA	Subordinate Message Transfer Agent
SMTP	Simple Mail Transfer Protocol
TCC	Telecommunications Center
TCP/IP	Transmission Control Protocol/Internet Protocol
TS/SCI	Request for Comments
UA	User Agent
USAF	United States Air Force
USMTF	US Message Text Format
WAN	Wide Area Network
WWW	World Wide Web (also called the Web)

APPENDIX B

REFERENCES

APPENDIX B: REFERENCES

USD(A) Memorandum, "Program Guidance on the Defense Message System (DMS)," 3 August 1988

Charter, Defense Message System (DMS) Implementation Group (DMSIG), Approved 22 August 1988

Charter, Defense Message System (DMS) Panel, Approved 22 August 1988

Joint Chiefs of Staff, MJCS-20-89, "Multi-command Required Operational Capability for the Defense Message System," MROC 3-88, 6 February 1989; Change 1, 4 August 1993

JS/J-6A 00395-93 Memo, "Subject: Defense Message System (DMS) Required Operational Messaging Characteristics (ROMC)," 4 May 1993; Change 1, 15 April 1994

Charter, Defense Message System (DMS) Program Manger (PM), Approved November 1994

Defense Message System Implementation Group, "The Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)," November 1994

Defense Message System, "CAPSTONE Test and Evaluation Master Plan," October 1994, Approved 12 May 95

OASD(C3I) Memorandum, "Electronic Mail (E-Mail) Policy," 13 October 1992

OASD Memorandum, "Elimination of Data Pattern Message Traffic from the Automatic Digital Network (AUTODIN)," 4 November 1992

OASD(C3I) Memorandum, "Interim Policy for Transition to the Defense Message System (DMS) Target Architecture," 2 November 1989

CJCSI 5721.01, Chairman of the Joint Chiefs of Staff Instruction, "The Defense Message System and Associated Message Processing Systems," 28 June 1993

OASD(C3I) Memorandum, "Electronic Messaging Policy - Implementation Guidance," 9 March 1995.

Allied Communications Publication (ACP) 123, November 1994

Defense Message System Home Page at URL -http://www.itsi.disa.mil/dmshome.html